How Three Poznan University Students Broke the German Enigma Code and Shortened World War Two

Roger G. Johnson

How three Poznan University students broke the German Enigma Code and shortened World War Two

Roger G Johnson [1]

[1] School of Computer Science, Birkbeck University of London, Malet Street, London WC1E 7HX, UK
rgj@dcs.bbk.ac.uk

Abstract. The story of the Allied breaking of the German Enigma codes in World War 2 was first published in the 1970s. Even now many of the details, especially concerning the critical work in the 1930s undertaken by gifted and dedicated Polish codebreakers remains largely unknown. Their work is credited with saving the Allies several years work and so shortening the war and saving thousands of lives. The holding of the IFIP World Computer Congress in Poznan, home of the Polish codebreakers, gave an opportunity for their work to be highlighted to an international audience. Talks covering the work of the Polish, British and French codebreakers were given and webcast worldwide. In addition, a encoded Enigma message was sent at the start of the day from Poznan to Bletchley Park in the UK where the volunteers of the Bombe team at The National Museum of Computing successfully confirmed their breaking of the message at the start of the afternoon session.

Keywords: Enigma, code breaking, World War II, Marian Rejevski, Jerzy Rozycki, Henryk Zygalski, Turing-Welchman Bombe

1 Background

In 1945 General Dwight D Eisenhower (Allied Supreme Commander Europe) wrote to General Stewart Menzies (Head of Bletchley Park in the UK saying that the successful reading of German messages had

"saved thousands of British and American lives and, in no small way, contributed to the speed with which the enemy was routed and eventually forced to surrender"

The story of how the Allied forces broke the German Enigma code during World War 2 has been told many times in recent years usually from a variety of perspectives mostly linked to Bletchley Park in the UK. The critical contribution of the Polish codebreakers remains little known outside Poland and only a limited number of books and papers have been published about their work. The Polish codebreakers repeatedly broke the Enigma code as its security features were steadily enhanced throughout the 1930s. The result was that as war was about to break out in 1939 the Poles were able to give

working replica Enigma machines to their French and British allies and to explain how they had successfully broken the German Enigma messages up to that time.

Without this dramatic gesture it is very unlikely that the British and French would have been able to develop the codebreaking techniques which enabled the British to read German Enigma traffic throughout most of World War 2 at Bletchley Park and also the French until late 1942 at Bletchley Park's French equivalent.

This paper summarises the story of the critical Polish contribution and how it was built on by the French and British, most notably by the British mechanisation of the most time-consuming part of finding the key each day by the building of machines which were named Bombes. The Polish role is well documented in two books, Kozaczuk (1984) first published in Polish in 1979 which focussed primarily on the codebreaking and very recently in Turing (2018) which recounts the codebreaking exploits but also the lives of the codebreakers during and after this tempestuous period.

The holding of the IFIP World Congress in Poznan in Poland provided an ideal opportunity for IFIP WG 9.7 on the History of Computing to celebrate the work of three talented and heroic Polish mathematics students from the University of Poznan, Marian Rejewski, Jerzy Rozycki and Henryk Zygalski, who trained in Poznan to become codebreakers and whose work ultimately led to the significant shortening of World War 2.

The author is a member of IFIP WG 9.7 and is also the Secretary of the Turing Welchman Bombe Rebuild Trust (TWBRT) which owns the replica Bombe completed in 2007 and is demonstrated every week at The National Museum of Computing (TNMoC) housed in Block H of Bletchley Park in the UK. He arranged for the TWBRT Bombe team to hold one of its occasional roadshow events in which an Enigma message is sent from a remote location to the Bombe Team at TNMoC who then attempt to break the code and send back confirmation of the message being successfully read.

2 Enigma Machine

The origins of the Enigma coding machine were with a commercial coding machine built by a German electrical engineer named Arthur Scherbius. He obtained several patents for his machines starting in 1918. The device evolved into a portable device about the size of a typewriter powered by batteries. Having initially failed to interest the German armed forces in his machine he sold them as commercial coding machines for use by financial institutions such as banks to protect commercially sensitive information being sent by telegraph and other devices. Turing [Turing 2018] records that in 1926 both the British and Polish authorities had obtained commercial examples to study while he also notes that, in the same year, German Navy signals using an Enigma machine are noted for the first time.

Following the largely static army operations of the First World War, military strategists developed ideas for future mobile land warfare. However, a critical issue would be to create effective communications for command and control of relatively small frontline military units. In addition, naval commanders, especially with a growing force of submarines, needed secure two-way communications to maintain contact with their forces. What was required was a secure coding machine which, given its presence close

to the frontline in mobile warfare, could sooner or later be captured by the enemy without compromising the security of the communications network. This need for portable, secure communications potentially across large distances, was the capability the Enigma machine provided. Figure 1 shows a German army Enigma machine.

Fig. 1. Three wheel Enigma machine

The key features of the Enigma machine were a conventional German keyboard and above it lamps which light each time a key is pressed with the enciphered character corresponding to the key pressed. Above the lamps are the three rotor wheels. Each time a key is depressed the righthand rotor advances one step and after one revolution the adjacent rotor advances one step and similarly with the leftmost rotor. Each rotor has the letters of the alphabet around the rim and every letter is wired to another letter elsewhere on the rotor. Thus a letter "A" typed on the keyboard may emerge from the first rotor as "K" and so on through the other two rotors. The electric current then reaches the plugboard on the front of the machine where 20 of the 26 letters are again wired up in pairs after which it returns through the wheels until it lights up a lamp on the machine. The Army Enigma machine ultimately had five rotors and on any day three would be used in a predefined arrangement of rotors. The result of all these different combinations is to produce over 150 million million million alternatives. A very comprehensive account of the evolution of the Enigma coding machine is provided in [Perera, 2010].

It was this extraordinary number of combinations which several times later in the war led the Germans to conclude, in the face of circumstantial evidence to the contrary such as dramatic increases in submarine losses after the Allied breaking of the naval

Enigma, that the Enigma machine had in fact not been broken but that there was an alternative explanation, such as espionage or allied technological advances, for significant German setbacks.

It is worth noting that other military powers, including Britain, also adopted coding machines which made use of rotors. It was fundamentally a good approach to automated enciphering of messages in an electro-mechanical era.

3 Poland and Germany

The inter-war Polish state was a creation of the Versailles Peace treaty. It was situated between Germany and Russia and the Polish authorities trusted neither. In the turmoil following the Russian revolution, the Polish government regarded the German state of the later 1920s as a bigger potential threat than the Soviet Union. Also Soviet codes were still using First World war techniques and so liable to successful attack.

Initial attempts to break German Enigma messages using the commercially available Enigma machine failed. Obviously the machine had been modified. Any attack on the machine would need trained cryptographers and so a special course was run at the University of Poznan which was in a part of Poland which had formerly been part of Germany and hence had many fluent German speakers. In 1929 20 students were recruited to the course. Further attempts at breaking into Enigma still yielded nothing until in 1932 the French recruited a spy, Hans-Thilo Schmidt, who worked as a civilian in the German Army's cryptography unit. To fund an extravagant life style he needed money and proceeded to sell large numbers of photographs of secret files relating to the work of the cryptographic unit to the French.

Unfortunately without a German military Enigma machine the French realised that the photographs of the operating instructions were of no immediate value. The British when offered the photographs came to the same conclusion. The French then approached the Poles who expressed more interest but asked for more information. Gradually through the first half of 1932 the French obtained more and more material from Hans-Thilo Schmidt until finally, in August 1932, they obtained an encrypted message together with the original text. With the other secret material already obtained, it now appeared that it might be possible to reverse engineer the Enigma machine, in particular the wiring of the rotors.

The first recruit to the Polish Cypher Bureau from the Poznan course was Marian Rejewski. Initially he worked on Enigma in the evening after his colleagues in the Cypher Bureau had gone home. Later on it became a full time but still secret project. Month by month he gradually worked out the wiring inside the machine. While for their part the French continued to supply more secret intelligence from Hans-Thilo Schmidt. The final problem to be overcome, once the wiring of the Enigma machine had been worked out was to determine a way to find which rotors were being used, in what order they had been placed into the machine and the starting position for each of the rotors. Marian Rejewski noticed that each message began with the starting position sent twice.

Fig. 2. Marian Rejevski, Jerzy Rozycki, Henryk Zygalski

Marian Rejevski was now joined by two more graduates of the Poznan course. They were Jerzy Rozycki and Henryk Zygalski. From the stolen operating instructions they knew that the Germans sent the starting position twice at the start of each message and they realised that during the encipherment almost certainly only the righthand wheel turned while the others remained stationery. Studying the patterns enabled them to devise simple lookup methods to find the arrangement of the rotors and also some of the plugboard settings. Further they realised that what they needed was a working copy of an Enigma machine. Starting with an old commercial machine as a model, the Poles constructed in utmost secrecy a small number of machines functionally the same as the then current German Enigma machine complete with correctly wired rotors and a plugboard.

The procedures used by the Germans continued to evolve. Gradually rotor orders were changed more frequently until in October 1936 they were changed daily. Sloppy operating practices were eliminated and more cables were used on the plugboard. A major change took place as war clouds gathered in 1938 when the Germans introduced two new rotors, making five in total, and changed their operating procedure to use a different initial wheel position for each message. Each time the Poles responded with new techniques to re-establish the setup of the machine so that messages could be successfully read.

4 Sharing with Britain and France

By 1938 both the British and French cryptographers had looked at approaches to breaking the Enigma messages but had made little progress with the latest German versions of the machine. They had only succeeded in breaking into simpler versions of Enigma used in the Spanish Civil War and also the less advanced Italian system.

The Munich crisis of 1938 caused both to examine their readiness for war which led to a substantial exchange of information about Enigma. The French knew from the intelligence they had supplied to the Poles that the Poles had probably made some progress but the British appear to have been unaware of the possible significance of the Polish work. However, the major changes by the German in late 1938 had stretched the

Polish resources close to breaking point. Their productivity in breaking into Enigma had dwindled dramatically.

In December 1938 the French proposed holding a three way conference in Paris between France, Britain and Poland at which the French hoped to find out what progress each had made. The meeting, held in January 1939, went badly with each party revealing only very limited amounts of information. However, it was clear to each party that the others were serious in their commitment to break into Enigma and so contacts were maintained through the spring and summer of 1939.

The next meeting was to be truly momentous but neither the British or French knew in advance. At the end of June 1939 the Poles, knowing through Enigma and other intelligence that Germany was preparing to invade Poland, invited the British and the French to Warsaw for a meeting. Thus it was in late July 1939 Alastair Denniston, Head of Bletchley Park and Dilly Knox, Britain's leading cryptographer and their principal expert on Enigma travelled across Nazi Germany by train to Poland. The French were represented by Gustav Bertrand, Denniston's opposite number and his deputy, Henri Braquenie. The Poles sent their trio of Rejewski, Rozycki and Zygalski together with their boss, Maksymilian Ciezki.

On the day following their arrival they were driven to the Poles' secret intelligence HQ at Pyry on the outskirts of Warsaw. To the amazement of the French and British the Poles announced almost immediately that they had broken Enigma some years earlier. The Poles showed them a variety of devices which they used to help determine each day's Enigma settings. Discussions continued next day as the Poles revealed more of their methods for breaking the code. However, without doubt, the highpoint was the offer by the Poles to donate to both the French and the British one of their precious working replica Enigma machines. The two machines left Poland by diplomatic bag for Paris and so, probably unnoticed by fellow travellers, Stewart Menzies, the Deputy Head of the British Secret Intelligence Service greeted Gustav Bertrand, the Head of the French Codebreakers as he arrived at Victoria Station in August 1939 with a large wooden box containing the priceless Enigma machine donated to the British.

At this point Alan Turing enters the story. He had been working part time on the Enigma problem at Cambridge since 1938 but had not made much progress. Following the Pyry meeting, Knox had shared with Turing all the information that the Poles had provided, including their mechanical devices for finding the key of the day. Very rapidly Turing conceived of an electro-mechanical machine to search for feasible solutions for the rotor starting positions based on a technique of guessing what the often stylised clear text of the German Enigma message might be. This specification for a machine was handed to BTM, the UK's leading punched card equipment manufacturer who were closely tied to IBM based in the USA, to turn into a physical reality.

A clear and full account of what became known as the Turing Welchman Bombe and how it was used is given in [Turing, 2014].

5 After the Polish invasion

On September 1st 1939 Germany invaded Poland and by the end of the month Polish resistance had collapsed. Poland was divided into three with large parts being assimilated by Germany in the west and the Soviet Union in the east with a small central area under the control of the Polish General Government. The Poles had planned for an invasion and destroyed evidence of their Enigma codebreaking work. It was vital that the codebreakers got away and so travelling by train and lorry they fled to Romania where they went first to the British Embassy who did not appreciate their significance and asked them to return the following day after the staff had contacted London. However, if they had been caught by the Romanian secret police they would probably be handed over to the Gestapo. Consequently, the Poles moved on immediately to the French Embassy who recognised their links with the French Secret Service and assisted them to reach France where they were met at the border by a representative sent by Gustav Bertrand. Knox and Denniston were not amused to find that the French had now got all the key Polish Enigma experts.

There followed a period of cooperation between Bletchley Park and the French codebreakers now established in the Chateau de Vignolles near Paris. The two groups were linked by a secure landline and from early 1940 there were daily races to find the Enigma key of the day. However, this period was not to last long. Early in May 1940 the German Army attacked the French and British forces in the West and on June 25th an armistice was signed between Germany and France. This divided France into two main areas – Occupied France in the north and "Free France" in the south with its government based in the small spa town of Vichy. From there, the Vichy government ran both Vichy France and also the whole of the worldwide French colonial empire.

In the anticipation that there might be an underground resistance movement within Vichy France, the armistice permitted the Vichy government to maintain a small codebreaking capability to track them down although they were expressly forbidden from intercepting German messages. Bertrand's group, including the Poles, moved to form this group now relocated to a small chateau outside Uzes near Nimes in southern France. The group now continued to intercept message traffic including German Enigma messages. Intelligence obtained, depending on its contents, could be passed to the Vichy authorities or to other groups. Bertrand's group built up a network of links across north Africa and Portugal supplying intelligence directly and through intermediaries to the British as well as De Gaulle's Free French and the Polish Government in exile in London and received equipment, finance and other benefits in exchange.

Assorted codebreakers travelled between the chateau at Uzes and north Africa to meet with other units working there. One of these trips ended in disaster when in January 1942 Jerzy Rozycki was drowned, when the ship on which travelling back to France from Algiers foundered in heavy seas with a substantial loss of life.

North Africa was in a very fluid state with many loose loyalties. In some places, such as Tangier, which had an international zone, officials as well as agents from many of the warring powers rubbed shoulders throughout the conflict. Fascinating insights into this period are to be found in [Pidgeon, 2008] which includes material on North Africa.

In November 1942, German and Italian forces took over Vichy France. The German authorities and their Vichy collaborators were closing in on the radio transmissions from the chateau. It was decided that the Poles should leave. The British concluded that the Poles were too numerous to be flown out. The other alternatives were to attempt an evacuation by sea, or overland via Switzerland or Spain. However the route into Switzerland was now effectively closed. Attempts to evacuate by sea proved too dangerous. Consequently in early January 1943 groups of Polish codebreakers began to travel across France towards the Pyrenees and the Spanish border. Marian Rejewski and Henryk Zygalski managed with some difficulty to cross the Spanish border together. In common with most undocumented entrants into Spain they were jailed by the Spanish authorities. However, as the German and Italian armies suffered reverses the attitude of the Spanish authorities softened. Finally, starting in April 1943 the prison camps were gradually emptied. Marian Rejewski and Henryk Zygalski were finally released and by stages travelled via Portugal and Gibraltar to the UK. Having regained their freedom they were once again part of the Polish armed forces. They were attached to a team based near Hemel Hempstead which worked on Russian codes for the remainder of the war.

When peace returned to Europe in May 1945, Marian Rejewski and Henryk Zygalski both faced a difficult choice, whether to return to Poland or to find a new home. Marian Rejewski had a wife and two small children in Poland and so he decided to return to his homeland. Returnees were often regarded with suspicion by the new communist authorities in Poland. Although his career as an accountant was interfered with by the authorities due to suspicions about his wartime work he survived to be honoured by Poland prior to his death in 1980 for his services to the defeat of Germany as the Polish political environment evolved. Henryk Zygalski in contrast had met a British girl during his wartime work in the UK. He became a British citizen and settled down to an academic career in the UK ultimately as a member of staff of the Mathematics Department of the University of Surrey. He remained in contact with Marian Rejewski until his death in 1978.

6 Celebration at WCC 2018

At the IFIP World Congress in Poznan in Poland IFIP WG 9.7 on the History of Computing held a stream on computing in eastern Europe. One of the most significant events of World War 2 was the breaking of the German Enigma codes. As noted earlier, the contribution of the British codebreakers has been widely described but the work of the Poles has been largely unacknowledged.

The Congress provided an opportunity to put right this omission. The day celebrated the work of three talented and heroic Polish mathematics students from the University of Poznan, Marian Rejewski, Jerzy Rozycki and Henryk Zygalski, who trained in Poznan to become codebreakers and whose work ultimately led to the significant shortening of World War 2. The event attracted significant media interest including TV and radio in both Poland and the UK. The event was also webcast and is currently available online [YouTube, 2018].

The one day Bombe stream comprised three lectures and a Bombe Roadshow challenge under the title of "Enigma Live", The opening talk was by Sir John Dermot Turing who asked the question "Did Alan Turing see an Enigma machine at Bletchley Park?". The second two talks were by Prof Marek Grajek from Poland. He spoke on the work of the Polish Codebreakers and secondly the proposed Poznan Enigma Centre one of whose main aims will be to promote the interest of young people in cryptography and computing.

Fig. 3. Turing Welchman Bombe used to break the Poznan message

The Bombe Roadshow was a challenge to decode an Enigma message using the Turing Welchman Bombe in the UK. This is a fully authentic replica of the machine originally designed by Alan Turing, enhanced by Gordon Welchman and built by BTM. It is regularly demonstrated at The National Museum of Computing housed in Block H at Bletchley Park in the UK by the Bombe team of volunteers. The Bombe's function was to find feasible wheel positions which is a critical and time consuming procedure in finding the key of the day. This process is fully explained in [Turing, 2014].

The plan for the event was to send, as an email attachment, an encrypted message with its clear equivalent (or "crib") followed by another encrypted message whose contents were unknown to the Bombe team. Due to a minor technical fault limiting the Bombe's operating speed it was necessary to send the crib message ahead of the event. Otherwise the day ran to plan and a successful break was made in the early afternoon when the decrypted message was sent to Poznan from the UK.

References

1. [Perera 2010] Inside Enigma by Tom Perera published by the Radio Society of Great Britain, 2010. ISBN 978 1 90508 664 1.
2. [Pidgeon, 2008] The Secret Communications War – The story of MI6 Communication 1939-1945 by Geoffrey Pidgeon published by Arundel Books, ISBN 978 0 95605 152 3.
3. [Turing 2014] Demystifying the Bombe by Dermot Turing published by The History Press, 2014, ISBN 978 1 84165 566 6.
4. [Turing 2018] X, Y and Z – The Real Story of How Enigma was Broken by Dermot Turing published by The History Press, 2018 ISBN 978 0 75098 782 0.
5. [YouTube 2018] Enigma Live webcast – eight talked including talks Dermot Turing and Marek Grajek, chaired by Roger G Johnson http://wcc2018.org/Enigma-live. Link checked January 1st 2019.